

December 15, 2000

Smart cards provide power and protection

Chip allows multiple applications, stores data to authenticate user

Consider these everyday activities. A woman buys a soft drink from a vending machine and gets cash from an ATM. She boards a commuter train. She takes a friend to lunch. She makes a long-distance call from a pay phone. She visits her doctor. But instead of using cash or a separate automatic teller card, transit pass, credit card, telephone card and health insurance card, she could make all the transactions with a single card—a smart card.

Such a scenario may soon become commonplace if smart cards catch on in the United States like they have in Europe. Most experts see a bright future for the cards, which carry an embedded computer chip and can perform many different functions. For corporate America, smart cards can enhance an overall security program.

Computers have revolutionized how Americans work, play and communicate. The Internet has opened up new vistas for commerce. With this technological revolution have come new security concerns. Companies want to protect their computer network from intruders and to control access to their property. E-commerce providers want to verify that a customer is who he or she claims to be. Private citizens want to protect their assets from identity thieves. The same technology that created the information superhighway also opened new roads for thieves and vandals. But technology also erects roadblocks to criminals. Smart cards are one such roadblock.

In recent months, *The Lipman Report* has focused on computer and Internet security. This focus reflects our conviction that as businesses harness the power and speed of computers, they must not neglect security precautions.

Smart cards offer ammunition in the war against computer-based crime. Development of the cards began in the late 1970s. Prodded by the French government because of fraud concerns, the French banking industry introduced smart cards in 1985 with an order of 16 million cards. France Telecom followed. In Germany, smart cards are used for storing national health insurance and medical records. At first, most of the cards were prepaid, disposable telephone cards, which are in use in the United States. More sophisticated uses followed.

United States lagged

Use of the cards spread through Europe, Asia and Latin America, but, until recently, the United States lagged. In 1999, about 1.5 billion smart cards were issued around the world. Only 19 million, or two percent, were issued in the United States. A product analyst for a technology company noted that major banks began test programs in several cities, but merchants complained that few customers used the cards. Customers preferred the familiar credit or debit cards with magnetic strips on the back.

That may be changing. In September, a major credit card company announced plans to introduce 10 million smart cards in the United States. Three large banks are ready to issue them to customers. The United States government is moving toward using smart cards as employee identification badges.

Multiple applications

Smart cards are plastic cards the size of credit cards with an embedded semiconductor that lets them accept, store and send information. Experts foresee a number of applications for the cards: identification, transportation, telecommunications, purchases and health care. Smart cards can hold thousands of times more data than magnetic-strip cards. The card can hold a memory chip, which only stores information, much like a magnetic card. Or it can hold a microprocessor, which can receive, store and process data. Smart cards can work in two ways. Contact cards must be inserted into card readers. Contactless cards use an antenna to receive a signal from the reader and must pass within a few inches of the reader to receive it. The signal also provides the card's power source.

Smart cards can store personal data, making it secure and portable, the product analyst noted. They are hacker resistant; a user must have a Personal Identification Number (PIN) or biometric identifier to get the card to perform. Smart cards are not limited to the typical four-digit PIN

(continued on next page)

Smart cards provide power and protection

Chip allows multiple applications, stores data to authenticate user

(continued from preceding page)

used with credit cards or ATM cards. The PIN could consist of ten digits, making it virtually impossible for a hacker to solve. And the PIN can be changed periodically.

Smart-card users will not need to memorize different passwords for different applications; they will carry the card instead. With multiple applications, the card is accepted at a variety of point-of-sale terminals, networks and databases. In each case, the card reader finds the pertinent data in the card's chip and processes the transaction. A smart card can offer varying levels of access to different parties. Some basic data would be accessible. More restricted data would require the user's private key. Some transactions would require the user's key and the other party's key in combination. For example, a smart health card could store a wealth of medical data. It could provide quick access to basic information such as the insurance company's name and emergency contacts. Retrieval of more detailed medical data on the cardholder would require an access key. The medical information could be updated after each visit to the doctor.

'Is it functional and reliable?'

A consultant to the smart card industry thinks Americans will quickly embrace multiple-application cards. "Consumers don't care about high-tech," he said. "They want to know, Is it functional and reliable?" He thinks versatility will be a key selling point: being able to use the same card for credit and debit functions, to rent cars and reserve plane tickets.

Smart cards provide internal security. "With multiple applications, there's an internal firewall between the different applications," the consultant said. A phone company, for example, could not look into a customer's bank account without an access key.

He noted the security benefits of smart cards as compared to magnetic-strip credit cards. A thief won't be able to get a smart card from a stolen

wallet and go on a buying spree. At the point of sale, the buyer must enter a PIN to activate the card. Merchants don't have to verify the smart card by calling a central database. Entry of the PIN demonstrates that the cardholder is who he or she claims to be.

Magnetic-strip cards are easy to duplicate. The chief information officer at a national company described a routine transaction. A waiter takes a restaurant patron's credit card. The few minutes required to process the charge give ample time to duplicate the credit card. But substitute a smart card in the restaurant scenario. First, the CIO points out, it cannot be duplicated. Second, it never leaves the patron's possession. A hand-held card reader is brought to the table and the patron enters a PIN. Of course, the failure to follow basic safeguards and use common sense can defeat any security system. The user must protect the PIN by memorizing it. The number should not be written on the card or carried in a wallet. The PIN should not duplicate easily accessible numbers such as addresses or phone numbers or birthdays.

Manufacturers are expecting the United States to follow in Europe's footsteps and embrace smart cards, mainly in the area of electronic commerce. In business, government, universities and private life, according to forecasters, people soon will use smart cards to log onto private computer networks or the Internet. Millions of employees and students will carry chip-based ID cards, which will replace passwords for computer access. An information security executive predicts that within 18 months the use of smart cards for computer access will increase from 5 percent to 30 percent of users.

Increasing levels of trust

Concern about on-line fraud is expected to boost smart card use. The cards can assure privacy, security and authentication for Internet transactions. Proponents say smart cards will increase electronic commerce by increasing levels of trust. The cards can connect sellers and buyers

by storing digital signatures, allowing sellers to establish the customer's identity. Because of the authentication and verification requirements of e-commerce, experts say, companies will be more willing to invest in the technology to support smart cards. Computer manufacturers will add smart-card readers to their products.

How quickly will the transition to smart-card technology occur? Magnetic-strip cards are replaced every 18 months and magnetic-strip readers every five years. Experts believe that the new cards and equipment can replace the old on the regular rotation, making acceptance by customers and merchants easier. Smart cards cost more than magnetic-strip cards, but may be more economical in the long run and are less prone to failure. "When you consider the cost per application," a consultant said, "the cost of a multi-application card drops below that of a magnetic-strip card. Plus they last twice as long and can be reprogrammed and updated."

The September announcement by a major credit card company involved the introduction of a low-priced multi-application smart card. The cards will have credit and debit capabilities, in the event that merchants begin using terminals that can read the cards. The cards will also store different levels of Internet security, from simple passwords for some transactions to digital signatures for more sensitive transactions.

Federal requirements that insurers and health care providers securely transmit electronic documents could boost smart cards, because they can carry digital certificates and encryption keys. A large New York-based bank plans to issue smart cards with digital certificates and encryption keys. These cards can authenticate customers for access to Web sites where they can make purchases and conduct other business online. This year, President William J. Clinton signed legislation that gave legal standing to digital signatures. Smart-card technology can provide the authorization and authentication.

'Smart' identification cards

The smart card also offers advantages as an identification card.

In October, the U.S. Department of Defense announced it would issue "smart" ID badges to its 4 million personnel worldwide. The department is considering using the card to process food service charges, store individual medical and dental records, and record data on training and rifle range performance.

An undersecretary of Defense said smart cards would revolutionize the way the Pentagon does business. By 2002, the card will become the standard ID for military personnel, some Reserve forces, civilian employees and even some outside contractors.

Similarly, corporations could use smart ID cards to control access to buildings and computer networks. The cards could store employee data such as work schedules or payroll information. Visitors could be issued smart cards that controlled what parts of the facility they could enter.

A corporate security expert said that a leading technology company plans to replace its proximity entry cards with smart cards and readers. To access the company's computer network, employees would insert the same smart card into slots in laptops or desktops. "Smart cards add another level of security," the expert said.

Biometric data boosts security

For higher levels of security needs, smart cards can contain photos or biometric data such as fingerprints, voice prints or retina scans.

In the Netherlands, customs officials are developing a system to check passports. A traveler's fingerprint is scanned and compared with a print on a smart card. There is no need to dial into a central database. In another system being tested in the Netherlands, smart-card technology may

(continued on next page)

Smart cards provide power and protection

Chip allows multiple applications, stores data to authenticate user

(continued from preceding page)

help nightclubs keep troublemakers out. A first-time customer enters a registration kiosk that scans a fingerprint and takes nine pictures of his or her face. The data is digitized and stored on a smart card, which is given to the customer. The process takes 10 seconds. On the next visit, the customer presents the card and is identified as the correct cardholder. A computer checks a database to see if the cardholder has a record of trouble. Those with a record may be refused entry. If the nightclub system is successful, it may be adapted to soccer stadiums, often the scene of violence, and theme parks.

Privacy concerns

The use of smart cards raises privacy concerns. An electronic privacy rights group worries that a smart card for employees could be too invasive, allowing the employer to track comings and goings and use of equipment. As with the issue of monitoring employee e-mail, an ethical company will try to balance legitimate business and security needs with an employee's privacy rights.

Similarly, the versatility of smart cards provokes concern about a possible national identification card. In 1999, a compromise between the U.S. House of Representatives and the Senate killed proposed federal standards for drivers' licenses and birth certificates. The lawmakers feared the standards could be the first step toward a national "smart" ID card, which citizens would have to produce in many contexts. The privacy rights group points out that smart cards could facilitate the collection of data about citizens' private behavior. The current system, in which citizens use different cards for different activities, is an obstacle to centralized data collection. Again, it is a question of balancing efficiency with privacy.

With proper safeguards, the smart card can be another weapon in the arsenal of a security-conscious company. Such a company wants to protect its human, material and intellectual assets.

Smart cards can help. The speed at which technology advances requires regular upgrades. Computer scientists strive to create new safeguards for equipment and software. Criminals work just as hard to defeat them. A company that runs in place will fall behind.

Computer chips have created paradoxes. Horizons expand while the world gets smaller. Equipment shrinks but its power and versatility soars. We have access to more information but threats to its security grow. According to experts, the time is right for smart cards. Proponents claim the cards will simplify everyday tasks.

A corporate security expert has become convinced that in addition to consumer benefits, smart cards offer substantial security benefits. "The data encryption on smart cards provides a higher level of security than any existing card access system," he said.

Proactive, innovative companies will see the benefits of the smart card for security. Identification badges can become more than a static record of name and photograph. Smart cards and readers can control access to property. They can replace passwords as a means of logging onto computers. And for merchants who deal with the public, either online or off, smart cards can authenticate that the buyer is who he or she claims to be.

Traditional security practices are as important as ever: pre-employment screening, drug testing, identification badges, controlled entry and a top-down focus on security. Smart cards for employees and clients build on this foundation. They can help a company do business efficiently without sacrificing security.

The benefits of portability, power and protection mean the day of the smart card is approaching. A forward-looking company will be ready.



The Lipman Report Editors